

図 5 に示した携帯電話機 100 の構成と異なる点は、まず、メモリカード 180 が装着されていること以外に、携帯電話機 101 は、公開暗号化キー K_Pp を保持して、再生モード時にキー K_Pp をデータバス B_S2 に出力する K_Pp 保持部 1524 を備える構成となっていることである。

さらに、携帯電話機 101 は、秘密復号キー K_p を保持する K_p 保持部 1520 と、この K_p 保持部 1520 から与えられるキー K_p に基づいて、データバス B_S2 を介してメモリカード 180 から与えられるキー K_Pp で暗号化されたセッションキー K_s1 を復号し抽出する復号処理部 1522 をさらに備える構成となっている。しかも、暗号化処理部 1504 は、この復号処理部 1522 から与えられるセッションキー K_s1 により、K_s 発生部 1502 からの自身のセッションキー K_s を暗号化してデータバス B_S2 に出力する。

携帯電話機 101 のその他の点は、図 5 に示した実施例 1 の携帯電話機 100 の構成の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

図 27 は、実施例 7 のメモリカード 180 に対応したコンテンツサーバ 11 の構成を示す概略ブロック図である。図 3 に示したコンテンツサーバ 10 の構成と異なる点は、データ処理部 310 における暗号化処理部 322 は、K_s 発生部 314 からのセッションキー K_s に基づいてではなく、携帯電話機に装着されたメモリカードからセッションキー K_s により暗号化されて送信され、復号処理部 318 により復号抽出されたセッションキー、たとえば、セッションキー K_s1 に基づいて、暗号化処理部 320 の出力をさらに暗号化して、データバス B_S1 を介して通信装置 350 に与える点である。

コンテンツサーバ 11 のその他の点は、図 3 に示した実施例 1 のコンテンツサーバ 10 の構成の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

図 28 は、本発明の実施例 7 のメモリカード 180 の構成を説明するための概略ブロック図であり、実施例 4 の図 18 と対比される関である。

メモリカード 180 の構成が、メモリカード 150 の構成と異なる点は、まず、セッションキー K_s1 発生部 1432 は、このカード独自のセッションキー K_s

1を発生することである。

メモリカード180は、さらに、カードという媒体に固有の公開暗号化キーK_P mediaを保持するK_P media保持部1440の出力と、データバスB_S3を介して携帯電話機101から与えられる公開暗号化キーK_P pとを受けて、

5 動作モードに応じていずれか一方を出力する切換えスイッチ1436を備える。切換えスイッチ1436は、接点P_iおよびP_hとを有し、接点P_iはデータバスB_S3と、接点P_hはK_P media保持部1440とそれ自身結合する。暗号化処理部1430は、切換えスイッチ1436から与えられる公開暗号化キーK_P mediaまたは公開暗号化キーK_P pのいずれかにより、K_s1発生部1

10 432からのセッションキーK_s1を暗号化して、データバスB_S3に与える。

すなわち、切換えスイッチ1436は、配信モードのとき、および移動モードにおいて移動先となっているときは、未使用状態であり、再生モードの時は、接点P_iの側に閉じておらず、移動モードにおいて移動元となっているときは、接点P_hの側に閉じている。

15 メモリカード180は、さらに、接点P_e、P_fおよびP_gを有し、復号処理部1404から与えられるコンテンツサーバ11からのセッションキーK_sと、K_s1発生部1432の出力と、データバスB_S4から与えられる携帯電話機101からのセッションキーK_sとを受けて、動作モードに応じていずれか1つを選択的に出力する切換えスイッチ1435を、切換えスイッチ1434の替わりに備える。接点P_eには復号処理部1404からの出力が、接点P_fにはK_s1発生部1432の出力が、接点P_gにはデータバスB_S4がそれぞれ結合している。したがって、暗号化処理部1406と復号処理部1410は、この切換えスイッチ1435から与えられるキーに基づいて、それぞれ、暗号化処理および復号処理を行なう。

20 25 すなわち、切換えスイッチ1435は、配信モードの場合にコンテンツサーバ11からのセッションキーの抽出を行なうときは、接点P_eの側に閉じておらず、配信モードの場合に配信サーバからの暗号化されたライセンスキーK_c、ライセンスIDデータL_i_c_e_n_s_e-ID、ユーザIDデータUser-IDについてキーK_s1による復号を行なうときは、接点P_fの側に閉じている。切換えスイ

5 チ 1 4 3 5 は、再生モードにおいて復号処理を行なうときは、接点 P f の側に閉じており、再生モードにおいて暗号化処理を行なうときは、接点 P g の側に閉じている。切換えスイッチ 1 4 3 5 は、移動モードにおいて移動元となっている場合に復号処理を行うときは、接点 P f の側に閉じており、移動モードにおいて移動元となっている場合に暗号化処理を行うときは、接点 P g の側に閉じている。
10 切換えスイッチ 1 4 3 5 は、移動モードにおいて移動先となっている場合に移動元のセッションキーを受け取るときは、接点 P e の側に閉じており、移動モードにおいて移動先となっている場合にライセンスキー K c 、ライセンス I D データ License - I D およびユーザ I D データ User - I D を受け取るときは、接点 P f の側に閉じている。

メモリカード 1 8 0 は、さらに、接点 P a 、 P b 、 P c および P e を有し、 K s 1 発生部 1 4 3 2 から与えられる自身のセッションキー K s 1 と、 K P c a r d 保持部 1 4 0 5 の出力と、データバス B S 5 から与えられるライセンスキー K c と、暗号化処理部 1 4 1 4 から与えられ、相手方の公開暗号化キー K P c a r d (n) により暗号化されたライセンスキー K c 、ライセンス I D データ License - I D およびユーザ I D データ User - I D とを受けて、動作モードに応じていずれか 1 つを選択的に出力する切換えスイッチ 1 4 0 9 を、切換えスイッチ 1 4 0 8 の替わりに備える。接点 P a には K s 1 発生部 1 4 3 2 からの出力が、接点 P b には K P c a r d 保持部 1 4 0 5 の出力が、接点 P c にはデータバス B S 5 が、接点 P d には暗号化処理部 1 4 1 4 の出力が、それぞれ結合している。したがって、暗号化処理部 1 4 0 6 は、この切換えスイッチ 1 4 0 9 から与えられるデータに対して、それぞれ、暗号化処理を行なう。

25 すなわち、切換えスイッチ 1 4 0 9 は、配信モードにおいて、配信先となっている場合にコンテンツサーバ 1 1 に自身の公開暗号化キー K P c a r d (1) や自身のセッションキー K s 1 を送信するときは、順次、接点 P b の側および接点 P a の側に閉じる。切換えスイッチ 1 4 0 9 は、再生モードのときは、接点 P c の側に閉じており、移動モードにおいて移動元となっているときは、接点 P d の側に閉じている。切換えスイッチ 1 4 0 9 は、移動モードにおいて移動先となっている場合にも移動元に自身の公開暗号化キー K P c a r d (1) や自身のセッ

ションキーK_s1を送信するときは、順次、接点P_bの側および接点P_aの側に閉じる。

図29は、図28で説明したメモリカード180を用いた配信モードを説明するためのフローチャートである。

5 図28においては、ユーザ1が、メモリカード180を用いることで、コンテンツサーバ11からコンテンツデータの配信を受ける場合の動作を説明している。

まず、ユーザ1の携帯電話機101から、ユーザのタッチキー1108の操作等によって、コンテンツサーバ11に対して配信リクエストがなされる（ステップS100）。

10 コンテンツサーバ11においては、この配信リクエストに応じて、セッションキー発生部314が、セッションキーK_sを生成する（ステップS103）。一方、メモリカード180の側では、K_s1発生部1432がセッションキーK_s1を生成する（ステップS103¹）。

15 コンテンツサーバ11では、続いて、コンテンツサーバ11内の暗号化処理部316が、公開暗号化キーK_Pmediaにより、セッションキーK_sを暗号化処理して、データバスBS1に与える（ステップS104）。

通信装置350は、暗号化処理部316からの暗号化セッションキー[K_s]K_{media}を、通信網を通じて、携帯電話機101のメモリカード180に対して送信する（ステップS106）。

20 メモリカード180においては、メモリインタフェース1200を介して、データバスBS3に与えられた受信データを、復号処理部1404が、秘密復号キーK_{media}により復号処理することにより、セッションキーK_sを復号し抽出する（ステップS108）。

25 続いて、配信モードにおいては、まず、切換えスイッチ1409が接点P_bが閉じる状態が選択されているので、暗号化処理部1406は、接点P_bを介してK_Pcard(1)保持部1405から与えられる公開暗号化鍵K_Pcard(1)（ユーザ1のメモリカードにおける公開暗号化鍵）を受け取り、続いて、切換えスイッチ1409が接点P_aが閉じる状態となって、暗号化処理部1406は、接点P_aを介してK_s1保持部1432から与えられるセッションキーK_s1を生成する（ステップS109）。

s 1を受け取る。暗号化処理部1406は、切換えスイッチ1435が接点P eが閉じる状態が選択されているので、復号処理部1404からのセッションキーK sにより、公開暗号化鍵K P c a r d (1)およびセッションキーK s 1を暗号化してデータバスB S 3に与える。

5 携帯電話機101は、暗号化処理部1406により暗号化されたデータ[K P c a r d (1)、K s 1]K sをコンテンツサーバ11に対して出力する(ステップS 1 1 2)。

10 サーバ31では、通信装置350により受信され、データバスB S 1に与えられたデータ[K P c a r d (1)、K s 1]K sを復号処理部318が、セッションキーK sにより復号化処理して、公開暗号化キーK P c a r d (1)およびセッションキーK s 1を復号抽出する(ステップS 1 1 4)。

15 続いて、配信制御部312は、ライセンスキーK cを配信情報データベース304より取得し(ステップS 1 1 6)。かつ、配信情報データベース304等に保持されているデータを元に、ライセンスIDデータL i c e n s e - I DおよびユーザIDデータUser - I D等のデータを生成する(ステップS 1 1 8)。

暗号化処理部320は、配信制御部312からのライセンスキーK c、ライセンスIDデータL i c e n s e - I DおよびユーザIDデータUser - I D等のデータを受取って、復号処理部318より与えられた公開暗号化キーK P c a r d (1)により暗号化処理する(ステップS 1 2 0)。

20 暗号化処理部322は、暗号化処理部320により暗号化されたデータを受取つて、さらにセッションキーK s 1により暗号化して、データバスB S 1に与える(ステップS 1 2 2)。

25 通信装置350は、暗号化処理部322により暗号化されたデータ[[K c, L i c e n s e - I D, User - I D]K c a r d (1)]K s 1をカード180に対して送信する。

カード180においては、切換えスイッチ1435が接点P fが閉じる状態が選択される状態に切換えられているので、復号処理部1410は、K s 1発生部1432からのセッションキーK s 1により、復号処理を行ない、データ[K c, L i c e n s e - I D, User - I D]K c a r d (1)を抽出し(ステップ

S 1 2 6) , メモリ 1 4 1 2 に格納する (ステップ S 1 2 8) 。

さらに、メモリカード 1 8 0においては、復号処理部 1 4 1 6が、メモリ 1 4 1 2 に格納されたデータ [K c , L i c e n s e - I D , U s e r - I D] K c a r d (1) を復号し、復号されたデータ L i c e n s e - I D , U s e r - I Dをコントローラ 1 4 2 0が、レジスタ 1 5 0 0に格納する (ステップ S 1 2 9) 。

一方、コンテンツサーバ 1 1 は、暗号化コンテンツデータ [D c] K c を配信情報データベース 3 0 4より取得して、通信装置 3 5 0を介して、メモリカード 1 8 0に送信する (ステップ S 1 3 0) 。

メモリカード 1 8 0においては、受信した暗号化コンテンツデータ [D c] K c をそのままメモリ 1 4 1 2 に格納する (ステップ S 1 3 2) 。

以上のような動作により、メモリカード 1 8 0は、コンテンツデータを再生可能な状態となる。

図 3 0 は、携帯電話機 1 0 1 内において、実施例 7 のメモリカード 1 8 0に保持された暗号化コンテンツデータから、コンテンツデータを復号化し、音楽として外部に出力するための再生モードを説明するフローチャートである。

図 3 0 を参照して、携帯電話機のタッチキー 1 1 0 8 等からのユーザ 1 の指示により、再生リクエストがメモリカード 1 8 0 に対して出力される (ステップ S 2 0 0) 。

メモリカード 1 8 0では、コントローラ 1 4 2 0がレジスタ 1 5 0 0からライセンス I Dデータ L i c e n s e - I D , ユーザ I Dデータ User - I D等を読み出す (ステップ S 2 0 5) 。

コントローラ 1 4 2 0は、復号化されたライセンス I Dデータ L i c e n s e - I D等に含まれる情報に基づいて、ライセンス I Dデータ L i c e n s e - I D中のデータにより指定されるコンテンツデータ (音楽データ) の再生処理の累算数が、再生可能回数の上限値を超えているかいないかを判断し (ステップ S 2 0 6) 、再生可能回数を超えていないと判断した場合は、携帯電話機 1 0 1のコントローラ 1 1 0 6にに対して、再生許可通知を送信する (ステップ S 2 0 8) 。

携帯電話機 1 0 1においては、まず、公開暗号化キー K P p をメモリカード 1 8 0に対して送信し、セッションキー発生回路 1 5 0 2がセッションキー K s を

生成する（ステップS210）。

一方、メモリカード180でもセッションキーKs1を生成し（ステップS210'）、公開暗号化キーKpでセッションキーKs1を暗号化して（ステップS211）、携帯電話機101に暗号化セッションキー[Ks1]Kpを送信する（ステップS212）。

携帯電話機101では、復号処理部1522が秘密復号キーKpにより、データバスBS2を介してメモリカード180から与えられた暗号化セッションキー[Ks1]Kpを復号し、セッションキーKs1を抽出し（ステップS213）、暗号化処理部1504が、セッションキーKs1によりセッションキーKsを暗号化して（ステップS214）、データバスBS2に暗号化セッションキー[Ks]Ks1が出力される（ステップS215）。

メモリカード180は、データバスBS3を介して、携帯電話機101により生成された暗号化セッションキー[Ks]Ks1を受け取り、セッションキーKs1により復号し、セッションキーKsを抽出する（ステップS216）。

さらに、メモリカード180は、再生処理が行われることに応じて、レジスター1500中のライセンスIDデータLicense-IDのうち、再生処理の累算数に関するデータを更新する（ステップ217）。

続いて、メモリカード180は、メモリ1412から、暗号化されているデータ[Kc, License-ID, User-ID]Kcard(1)を読み出し、復号処理部1416が復号してライセンスキーKcを抽出する（ステップS218）。

続いて、抽出したセッションキーKsにより、ライセンスキーKcを暗号化し（ステップS219）、暗号化ライセンスキー[Kc]KsをデータバスBS2に与える（ステップS220）。

携帯電話機101の復号処理部1506は、セッションキーKsにより復号化処理を行なうことにより、ライセンスキーKcを取得する（ステップS222）。

続いて、メモリカード180は、暗号化コンテンツデータ[Dc]Kcをメモリ1412から読み出し、データバスBS2に与える（ステップS224）。

携帯電話機の音楽再生部1508は、暗号化コンテンツデータ[Dc]Kcを、

抽出されたライセンスキーK_cにより復号処理し(ステップS226)、コンテンツデータを再生して混合部1510に与える(ステップS228)。

一方、ステップS206において、コントローラ1420が復号処理は不可能であると判断した場合、メモリカード180は、携帯電話機101に対して、再生不許可通知を送信する(ステップS230)。

以上のような構成とすることで、メモリカードおよび携帯電話機が独自のセッションキーを生成する場合でも、ユーザがコンテンツデータを再生できる回数を制限することが可能である。

図31は、実施例7の2つのメモリカード間において、コンテンツデータおよびキーデータ等の移動を行なう処理を説明するためのフローチャートである。

図31を参照して、まず、図31においては、携帯電話機101が送信側であり、これと同様の構成を有する携帯電話機103が受信側であるものとする。また、携帯電話機103にも、メモリカード180と同様の構成を有するメモリカード182が装着されているものとする。

携帯電話機101は、まず、自身の側のメモリカード180と、受信側の携帯電話機103に挿入されたメモリカード182に対して、移動リクエストを出力する(ステップS300)。

これに応じて、携帯電話機101においては、メモリカード180内のセッションキー発生回路1432は、セッションキーK_s1を生成し(ステップS312)、一方、携帯電話機103においては、メモリカード182内のセッションキー発生回路1432は、セッションキーK_s2を生成する(ステップS312')。

携帯電話機101においては、メモリカード180は、公開暗号化キーK_{Pub}を用いて、暗号化処理部1430がセッションキーK_s1を暗号化して(ステップS314)、たとえば、トランシーバモードではアンテナ1102を介して、暗号化セッションキー[K_s]K_{Pub}をメモリカード182に伝達する(ステップS316)。

メモリカード182においては、復号処理部1404が、秘密復号キーK_{Sec}により、セッションキーK_s1を復号抽出し(ステップS320)、さら

に、セッションキーK_s1によりメモリカード182の公開暗号化キーK_{P c a r d}(2)およびセッションキーK_s2を暗号化して(ステップS322)、メモリカード180に対して、暗号化されたデータ[K_{P c a r d}(2)、K_s2]K_s1を送信する(ステップS324)。

5 メモリカード180においては、メモリカード182から送信された暗号化データを復号処理部1410がセッションキーK_s1により復号化して、メモリカード182の公開暗号化キーK_{P c a r d}(2)およびセッションキーK_s2を復号抽出する(ステップS326)。このとき、切換えスイッチ1435では接点P_fが閉じておおり、K_s1発生回路1432からのキーK_s1が復号処理部1410に与えられている。

続いて、メモリカード180においては、メモリ1412からメモリカード150の公開暗号化キーK_{c a r d}(1)により暗号化されているライセンスキーK_c、ライセンスIDデータL_{i c e n s e}-IDおよびユーザIDデータUser-IDが読み出される(ステップS328)。

15 続いて、復号処理部1416が、秘密復号キーK_{c a r d}(1)により、ライセンスキーK_c、ライセンスIDデータL_{i c e n s e}-ID、ユーザIDデータUser-IDとを復号処理する(ステップS330)。

コントローラ1420は、このようにして復号されたライセンスキーK_c、ライセンスIDデータL_{i c e n s e}-ID、ユーザIDデータUser-IDの値を、レジスタ1500内のデータ値と置換する(ステップS331)。

さらに、暗号化処理部1414は、復号処理部1410において抽出されたカード182における公開暗号化キーK_{P c a r d}(2)により、ライセンスキーK_c、ライセンスIDデータL_{i c e n s e}-ID、ユーザIDデータUser-IDとを暗号化する(ステップS332)。

25 暗号化処理部1414により暗号化されたデータは、切換えスイッチ1409(接点P_dが閉じている)を介して、さらに、暗号化処理部1406に与えられ、暗号化処理部1406は、データ[K_c、L_{i c e n s e}-ID、User-ID]K_{c a r d}(2)をメモリカード182のセッションキーK_s2により暗号化する(ステップS334)。このとき、切換えスイッチ1435は、接点P_g

が閉じており、復号処理回路 1410 からのセッションキー K_{s2} が暗号化処理部 1406 に与えられている。

続いて、メモリカード 180 は、携帯電話機 101 を介して、メモリカード 182 に対して、暗号化されたデータ $[[K_c, \text{License-1D}, \text{User-1D}] \text{Card} (2)] K_{s2}$ を送信する (ステップ S 336)。

メモリカード 182 においては、メモリカード 180 から送信されたデータを復号処理部 1410 により、セッションキー K_{s2} に基づいて復号化処理して、メモリ 1412 に格納する (ステップ S 339)。さらに、メモリカード 182 は、ライセンスキー $K_{card} (2)$ に基づいて、データ $[K_c, \text{License-1D}, \text{User-1D}] \text{Card} (2)$ を復号し、復号されたライセンス 1D データ License-1D 、ユーザ 1D データ User-1D をレジスタ 1500 に格納する (ステップ S 341)。

一方、メモリカード 180 は、さらに、レジスタ 1500 に格納されたライセンス 1D データ License-1D およびユーザ 1D データ User-1D を消去する (ステップ S 343)。

続いて、メモリカード 180 は、暗号化コンテンツデータ $[D_c] K_c$ をメモリから読み出し、メモリカード 182 に対して送信する (ステップ S 344)。

メモリカード 182 は、受信した暗号化コンテンツデータをそのままメモリ 1412 に格納する (ステップ S 346)。

以上のような処理を行なうと、ステップ S 342 において、ライセンスキー K_c 、ライセンス 1D データ License-1D およびユーザ 1D データ User-1D 等がメモリカード 180 からは消去されているので、メモリカード 180 は「状態 S B」となる。

一方、メモリカード 182 においては、暗号化コンテンツデータ以外にも、ライセンスキー K_c 、ライセンス 1D データ License-1D 、ユーザ 1D データ User-1D 等のすべてのデータが移動されているので、メモリカード 182 は「状態 S A」となっている。

以上のような構成を用いることで、たとえば、メモリカード 180 からメモリカード 182 へのデータの移動を、上述したようなセッションキー発生回路 15

0.2を有する携帯電話機を介さずに、メモリカードとメモリカードとを接続可能なインターフェース機器により行なうことも可能となり、ユーザの利便性が一層向上するという効果がある。

しかも、ライセンスIDデータL i c e n s e - I D等は、レジスタ1500に格納され、コントローラ1420はそれを参照すればよいため、動作に必要な処理量を低減できる。

さらに、セッションキーが、携帯電話機、メモリカードの各々で異なるため、通信のセキュリティーが一層向上する。

ここで、移動時には、再生情報内の再生回数を制限するライセンスIDデータL i c e n s e - I Dについては、メモリ1412に記録されたライセンスIDデータL i c e n s e - I Dを、レジスタ1500にて再生の都度修正された再生回数を記録したライセンスIDデータL i c e n s e - I Dに変更して、新たな再生情報を構成する。このようにして、メモリカード間をコンテンツデータが移動しても、再生回数に制限があるコンテンツデータの再生回数は、配信時に決められた再生回数の制限を越えることがないようにすることが可能である。

[実施例8]

実施例8の携帯電話機105およびメモリカード190は、以下に説明するように、実施例7の携帯電話機101およびメモリカード180の構成とは、以下の点で異なることを特徴とする。

すなわち、実施例8の携帯電話機105では、たとえば、あらかじめ配信システムにおける認証機構等の管理部門にこの携帯電話機105を登録する際に、この携帯電話機105に割当てられた公開暗号化鍵K P p および認証データC r t fとを公開復号鍵（公開認証鍵）K P m a s t e rにより暗号化された形で記録保持する手段を有している。

同様に、実施例8のメモリカード190でも、たとえば、あらかじめ配信システムにおける認証機構等の管理部門にこのメモリカード190を登録する際に、このメモリカードに割当てられた公開暗号化鍵K P m e d i a および認証データC r t fとを公開復号鍵（公開認証鍵）K P m a s t e rにより暗号化された形で記録保持する手段を有している。

ここで、メモリカード190および実施例8のコンテンツサーバ12には、この公開復号鍵（公開認証鍵）KPmasterを記録保持する手段を有している。この公開復号鍵（公開認証鍵）KPmasterは、システム中でデータ出力を行なう全ての機器がセッションキーにやりとりに対しても、相互にデータの授受を行なえる機器であることの証明と、セッションキーを相手方に送付する際に用いる暗号鍵の獲得に用いるシステム共通の鍵である。

以下、さらに、実施例8の携帯電話機105、メモリカード190およびコンテンツサーバ12の構成をより詳しく説明する。

図32は、実施例8における携帯電話機105の構成を説明するための概略ブロック図である。

図26に示した携帯電話機101の構成と異なる点は、KPp保持部1524の替わりに、公開復号鍵（公開認証鍵）KPmasterにより暗号化された、公開暗号鍵KPpおよび認証データCrtfを保持するための[KPp, Crtf]KPmaster保持部1525を備える構成となっていることである。

携帯電話機105のその他の点は、図26に示した実施例7の携帯電話機101の構成の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

図33は、実施例8のメモリカード190に対応したコンテンツサーバ12の構成を示す概略ブロック図である。図27に示したコンテンツサーバ11の構成と異なる点は、データ処理部310は、公開復号鍵KPmasterを保持するKPmaster保持部324と、KPmaster保持部324から出力される公開復号キーKPmasterに基づいて、通信網から通信装置350を介してデータバスBS1に与えられるデータを復号するための復号処理部326とをさらに備える構成となっている点である。暗号化処理部316は、復号処理部326での復号処理により抽出された公開暗号化キーKPmediaにより、Ks発生部314で発生されたセッションキーKsを暗号化し、また、配信制御部312は、復号処理部326での復号処理により抽出された認証データCrtfにより、配信を求めてきたメモリカードが正規のメモリカードであるかの認証を行なう。

コンテンツサーバ1-2のその他の点は、図2-7に示した実施例7のコンテンツサーバ1-1の構成の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

5 図3-4は、本発明の実施例8のメモリカード1-9-0の構成を説明するための概略ブロック図であり、実施例7の図2-8と対比される図である。

実施例8のメモリカード1-9-0の構成が、実施例7のメモリカード1-8-0の構成と異なる点は、まず、メモリカード1-9-0は、公開暗号鍵K_Pmediaおよび証明データCrtfとを公開復号鍵（公開認証鍵）K_Pmasterにより暗号化された形で記録保持する[K_Pmedia, Crtf] K_Pmaster保持部1-4-4-2を備える構成となっていることである。一方で、切換えスイッチ1-4-3-6は省略され、[K_Pmedia, Crtf] K_Pmaster保持部1-4-4-2の出力は直接データバスBS-3に与えられる。

さらに、メモリカード1-9-0は、公開復号鍵K_Pmasterを記録保持するためのK_Pmaster保持部1-4-5-0と、K_Pmaster保持部1-4-5-0から出力される公開復号キーK_Pmasterに基づいて、データバスBS-3上のデータを復号するための復号処理部1-4-5-2とを備える。

20 復号処理部1-4-5-2での復号処理により抽出される公開暗号化鍵K_Pmediaおよび認証データCrtfのうち、公開暗号化鍵K_Pmediaは、暗号化処理部1-4-3-0に与えられ、認証データCrtfは、データバスBS-5を介して、コントローラ1-4-2-0に与えられる。

メモリカード1-9-0のその他の構成は、図2-8に示したメモリカード1-8-0の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

図3-5は、図3-4に示したメモリカード1-9-0内の記録空間の構成を示す概略図である。メモリカードが独自に管理して、ユーザーが自由にその内容を書きかえることも読み出すこともできず、かつ、不当な開封処理に対しては、内部のデータが破壊されるTRMモジュールにより構成されるセキュリティ領域1-4-9-0、ユーザーからデータの存在は確認できるものの、そのデータがメモリカード固有の暗号化、ここでは公開暗号化鍵K_Pcard(1)による暗号化が施され記録され、データの書き換えが自由に行なえない準セキュリティ領域1-4-9-1と、ユ

一ザがその内容を自由に読み出し、書き換えが行なえる非セキュリティー領域 1492とを備える。

セキュリティー領域1490には、メモリカード190の出荷時から保持する鍵の保持部、すなわち、Kmedia保持部1402、KPCard(1)保持部1405、Kcard(1)保持部1415、[KPmedia、Crtf]KPMaster保持部1442、KPMaster保持部1450と、平文のライセンス情報が格納されるレジスタ1500が設けられる。

準セキュリティー領域1491には、メモリカード1900固有の暗号化をされたデータである[Kc, License-ID, User-ID]Kcard(1)が格納され、メモリ1412内に設けられる。

非セキュリティー領域1493には、暗号化コンテンツデータ[Dc]Kcが格納され、メモリ1412内に設けられる。したがって、暗号化コンテンツデータ[Dc]Kcは自由に複製することが可能となるが、再生に必要なデータが複製できない構成になっている。準セキュリティー領域1491に格納されたライセンス情報を他のメモリカードに複製しても、メモリカード1900の固有の公開暗号鍵KPCard(1)にてかけられた暗号化は、対の秘密復号鍵Kcard(1)を持たない他のメモリカードでは複製できないからである。

また、鍵を保持する全ての鍵保持部をセキュリティー領域に設けるよう説明したが、秘密復号鍵を保持するKmedia保持部1402およびKcard(1)保持部1415のみセキュリティー領域に配置さえすれば良く、他の鍵保持部に保持された鍵は外部より参照できるROM(Read Only Memory)に配置されていてもよい。

図36は、図35で説明したメモリカード190を用いた配信モードを説明するためのフローチャートである。

図36においては、ユーザ1が、メモリカード190を用いることで、コンテンツサーバ12からコンテンツデータの配信を受ける場合の動作を説明している。

まず、ユーザ1の携帯電話機105から、ユーザのタッチキー1108の操作等によって、メモリカード190に対して配信リクエストがなされる(ステップS400)。

メモリカード190からは、[KPmedia, Crtf]KPmaster保持部1442から、携帯電話機105を経由して、コンテンツサーバ12に対して、暗号化データ[KPmedia, Crtf]KPmasterが送信される（ステップS402）。

5 コンテンツサーバ12においては、暗号化データ[KPmedia, Crtf]KPmasterを受信すると、KPmaster保持部324が保持する公開復号キーKPmasterに基づいて、復号処理部326が復号処理することにより、公開暗号化キーKPmediaおよび認証データCrtfを取得する（ステップS404）。

10 さらに、コンテンツサーバ12においては、認証データCrtfによりメモリカード190の認証を行ない（ステップS406）、メモリカード190が正規のメモリカードであることが証明されれば、処理はS412に移行する。一方、コンテンツサーバ12は、メモリカード190が正規のメモリカードであることが証明されない場合は、配信不許可通知を送信し（ステップS408）、携帯電話機105が配信不許可通知を受信する（ステップS410）。

メモリカード190が正規のメモリカードであることが証明された場合、コンテンツサーバ12では、セッションキー発生部314が、セッションキーKsを生成する（ステップS412）。

15 コンテンツサーバ12では、続いて、コンテンツサーバ12内の暗号化処理部316が、公開暗号化キーKPmediaにより、セッションキーKsを暗号化処理して、データバスBS1に与える（ステップS414）。

通信装置350は、暗号化処理部316からの暗号化セッションキー[Ks]Kmediaを、通信網を通して、携帯電話機105のメモリカード190に対して送信する（ステップS416）。

20 メモリカード190においては、メモリインターフェースL200を介して、データバスBS3に与えられた受信データを、復号処理部1404が、秘密復号キーKmediaにより復号処理することにより、セッションキーKsを復号し抽出する（ステップS418）。さらに、メモリカード190では、Ks1発生部1432がセッションキーKs1を生成する（ステップS420）。

統いて、配信モードにおいては、まず、切換えスイッチ 1409 が接点 P b が閉じる状態が選択されているので、暗号化処理部 1406 は、接点 P b を介して K P c a r d (1) 保持部 1405 から与えられる公開暗号化鍵 K P c a r d (1) を受け取り、統いて、切換えスイッチ 1409 が接点 P a が閉じる状態となつて、暗号化処理部 1406 は、接点 P a を介して K s 1 発生部 1432 から与えられるセッションキー K s 1 を受け取る。暗号化処理部 1406 は、切換えスイッチ 1435 が接点 P e が閉じる状態が選択されているので、復号処理部 1404 からのセッションキー K s により、公開暗号化鍵 K P c a r d (1) およびセッションキー K s 1 を暗号化してデータバス B S 3 に与える (ステップ S 4 22)。

携帯電話機 105 を介して、暗号化処理部 1406 により暗号化されたデータ [K P c a r d (1)、K s 1] K s がコンテンツサーバ 12 に対して送信される (ステップ S 4 24)。

コンテンツサーバ 12 では、通信装置 350 により受信され、データバス B S 1 に与えられたデータ [K P c a r d (1)、K s 1] K s を復号処理部 318 が、セッションキー K s により復号化処理して、公開暗号化キー K P c a r d (1) およびセッションキー K s 1 を復号抽出する (ステップ S 4 26)。

統いて、配信制御部 312 は、ライセンスキー K c を配信情報データベース 304 より取得し (ステップ S 4 28)、かつ、配信情報データベース 304 等に保持されているデータを元に、ライセンス ID データ L i c e n s e - I D およびユーザ ID データ User - I D 等のデータを生成する (ステップ S 4 30)。

暗号化処理部 320 は、配信制御部 312 からのライセンスキー K c 、ライセンス ID データ L i c e n s e - I D およびユーザ ID データ User - I D 等のデータを受取って、復号処理部 318 より与えられた公開暗号化キー K P c a r d (1) により暗号化処理する (ステップ S 4 32)。

暗号化処理部 322 は、暗号化処理部 320 により暗号化されたデータを受取つて、さらにセッションキー K s 1 により暗号化して、データバス B S 1 に与える (ステップ S 4 34)。

通信装置 350 は、暗号化処理部 322 により暗号化されたデータ [[K c 、

L i c e n s e - I D, U s e r - I D] K e a r d (1)] K s 1をメモリカ
ード190に対して送信する (ステップS436)。

メモリカード190においては、切換えスイッチ1435が接点P1が閉じる
状態が選択される状態に切換えられているので、復号処理部1410は、Ks1
5 発生部1432からのセッションキーKs1により、復号処理を行ない、データ
[Kc, L i c e n s e - I D, U s e r - I D] K e a r d (1) を抽出し
(ステップS438)、メモリ1412に格納する (ステップS440)。

さらに、メモリカード190においては、復号処理部1416が、メモリ14
10 12に格納されたデータ [Kc, L i c e n s e - I D, U s e r - I D] K
e a r d (1) を復号し、復号されたデータL i c e n s e - I D, U s e r - I
Dをコントローラ1420が、レジスタ1500に格納する (ステップ442)。

一方、コンテンツサーバ12は、暗号化コンテンツデータ [Dc] Kcを配信
情報データベース304より取得して、通信装置350を介して、メモリカード
180に送信する (ステップS444)。

メモリカード190においては、受信した暗号化コンテンツデータ [Dc] K
cをそのままメモリ1412に格納する (ステップS446)。

以上のような動作により、メモリカード190は、コンテンツデータを再生可
能な状態となる。

図37は、携帯電話機105内において、実施例8のメモリカード190に保
持された暗号化コンテンツデータから、コンテンツデータを復号化し、音楽と
して外部に出力するための再生モードを説明するフローチャートである。

図37を参照して、携帯電話機のキーボード1108等からのユーザ1の指示
により、再生リクエストが携帯電話機105に与えられると (ステップS50
0)、携帯電話機105からメモリカード190に対して暗号化データ[KPp,
25, C r t f] K P m a s t e r が送信される (ステップS502)。

メモリカード190では、復号処理部1452での公開復号キーK P m a s
t e rによる復号処理により、公開暗号化鍵KPpおよび認証データC r t fが取
得される (ステップS504)。コントローラ1420は、認証データC r t f
により携帯電話機105が正規の機器であるかを認証し (ステップS506)、

正規の機器であると証明されると、処理をステップS 508に移行し、正規の機器であると証明されないと再生不許可の通知を携帯電話機105に対して送信する（ステップS 544）。

携帯電話機105が正規の機器であると証明された場合（ステップS 506）、
5 セッションキー発生部1432がセッションキーKs1を生成する（ステップS 508）。暗号化処理部1430は、復号処理部1452からの公開暗号化キーKpに基づいて、セッションキーKs1を暗号化し（ステップS 510）、暗号化セッションキー[Ks1]Kpがメモリカード190から携帯電話機105に対して送信される（ステップS 512）。

10 携帯電話機105では、復号処理部1522での復号処理により、セッションキーKs1が復号され抽出される（ステップS 514）。続いて、セッションキー発生部1502においてセッションキーKsが生成され（ステップS 516）、暗号化処理部1504がセッションキーKs1によりキーKsを暗号化して（ステップS 518）、携帯電話機105からメモリカード190に対して、暗号化セッションキー[Ks]Ks1が送信される（ステップS 520）。

15 メモリカード190では、復号処理部1410がセッションキーKs1により、暗号化セッションキー[Ks]Ks1を復号処理してセッションキーKsを抽出する（ステップS 522）。さらに、メモリカード190では、コントローラ1420がレジスター1500からライセンスIDデータLicense-ID、ユーザIDデータUser-ID等を読み出す（ステップS 524）。

20 コントローラ1420は、復号化されたライセンスIDデータLicense-ID等に含まれる情報に基づいて、ライセンスIDデータLicense-ID中のデータにより指定されるコンテンツデータ（音楽データ）の再生処理の累算数が、再生可能回数の上限値を超えていたかを判断し（ステップS 526）、再生可能回数を超えていないと判断した場合は、メモリカード190は、再生処理が行われることに応じて、レジスター1500中のライセンスIDデータLicense-IDのうち、再生処理の累算数に関するデータを更新する（ステップS 528）。

統いて、メモリカード190は、メモリ1412から、暗号化されているデータ

タ [Kc, License-ID, User-ID] K card (1) を読み出し、
復号処理部 1416 が復号してライセンスキー Kc を抽出する (ステップ S 530)。

5 続いて、ステップ S 522 において抽出したセッションキー Ks により、ライセンスキー Kc を暗号化し (ステップ S 532)。暗号化ライセンスキー [Kc] Ks をデータバス BS2 に与える (ステップ S 534)。

携帯電話機 105 の復号処理部 1506 は、セッションキー Ks により復号化処理を行なうことにより、ライセンスキー Kc を取得する (ステップ S 536)。

10 続いて、メモリカード 190 は、暗号化コンテンツデータ [Dc] Kc をメモリ 1412 から読み出し、データバス BS2 に与える (ステップ S 538)。

携帯電話機の音楽再生部 1508 は、暗号化コンテンツデータ [Dc] Kc を、抽出されたライセンスキー Kc により復号処理し (ステップ S 540)、コンテンツデータを再生して混合部 1510 に与える (ステップ S 542)。

一方、ステップ S 526 において、コントローラ 1420 が復号処理は不可能であると判断した場合、メモリカード 190 は、携帯電話機 105 に対して、再生不許可通知を送信する (ステップ S 544)。

以上のような構成とすることで、メモリカードおよび携帯電話機が独自のセッションキーを生成する場合でも、ユーザがコンテンツデータを再生できる回数を制限することが可能である。

20 図 3-8 は、実施例 8 の 2 つのメモリカード間において、コンテンツデータおよびキーデータ等の移動を行なう処理を説明するためのフローチャートである。

図 3-8 を参照して、まず、図 3-8 においては、携帯電話機 105 が送信側であり、これと同様の構成を有する携帯電話機 107 が受信側であるものとする。また、携帯電話機 107 にも、メモリカード 190 と同様の構成を有するメモリカード 192 が装着されているものとする。

携帯電話機 105 は、まず、受信側の携帯電話機 107 に挿入されたメモリカード 192 に対して、移動リクエストを出力する (ステップ S 600)。

これに応じて、携帯電話機 107 に装着されたメモリカード 192 からは、メモリカード 190 に対して、暗号化データ [K P m e d i a, C r t f] K P m a

st er が送信される (ステップ S 6 0 2)。

メモリカード 1 9 0においては、暗号化データ [K P m e d i a, C r t f] K P m a s t e r を受信すると、K P m a s t e r 保持部 1 4 5 0 が保持する公開復号キー K P m a s t e r に基づいて、復号処理部 1 4 5 2 が復号処理することにより、公開暗号化キー K P m e d i a および認証データ C r t f を取得する (ステップ S 6 0 4)。

さらに、メモリカード 1 9 0においては、認証データ C r t f によりメモリカード 1 9 2 の認証を行ない (ステップ S 6 0 6)、メモリカード 1 9 2 が正規のメモリカードであることが証明されれば、処理は S 6 1 2 に移行する。一方、メモリカード 1 9 0 は、メモリカード 1 9 2 が正規のメモリカードであることが証明されない場合は、移動不許可通知を送信し (ステップ S 6 0 8)、携帯電話機 1 0 7 が移動不許可通知を受信する (ステップ S 6 1 0)。

メモリカード 1 9 2 が正規のメモリカードであることが証明された場合、メモリカード 1 9 0 では、セッションキー発生部 1 4 3 2 が、セッションキー K s 1 を生成する (ステップ S 6 1 2)。

メモリカード 1 9 0 では、続いて、暗号化処理部 1 4 3 0 が、公開暗号化キー K P m e d i a により、セッションキー K s 1 を暗号化処理して、データバス B S 3 に与える (ステップ S 6 1 4)。

メモリカード 1 9 0 からは、暗号化処理部 1 4 3 0 からの暗号化セッションキー [K s] K m e d i a を、携帯電話機 1 0 5 を通じて、携帯電話機 1 0 7 のメモリカード 1 9 2 に対して送信する (ステップ S 6 1 6)。

メモリカード 1 9 2 においては、メモリインターフェース 1 2 0 0 を介して、データバス B S 3 に与えられた受信データを、復号処理部 1 4 0 4 が、秘密復号キー K m e d i a により復号処理することにより、セッションキー K s を復号し抽出する (ステップ S 6 1 8)。さらに、メモリカード 1 9 2 では、K s 1 発生器 1 4 3 2 と同様の構成を有する K s 2 発生部 1 4 3 2 ' がセッションキー K s 2 を生成する (ステップ S 6 2 0)。

続いて、メモリカード 1 9 2 では、まず、切換えスイッチ 1 4 0 9 が接点 P b が閉じる状態が選択されているので、暗号化処理部 1 4 0 6 は、接点 P b を介し

て K P c a r d (1) 保持部 1 4 0 5 から与えられる公開暗号化鍵 K P c a r d (1) を受け取り、続いて、切換えスイッチ 1 4 0 9 が接点 P a が閉じる状態となって、暗号化処理部 1 4 0 6 は、接点 P a を介して K s 2 発生部 1 4 3 2 から与えられるセッションキー K s 2 を受け取る。暗号化処理部 1 4 0 6 は、切換えスイッチ 1 4 3 5 が接点 P e が閉じる状態が選択されているので、復号処理部 1 4 0 4 からのセッションキー K s 1 により、公開暗号化鍵 K P c a r d (1) およびセッションキー K s 2 を暗号化してデータバス B S 3 に与える (ステップ S 6 2 2)。

10 携帯電話機 1 0 7 を介して、暗号化処理部 1 4 0 6 により暗号化されたデータ [K P c a r d (1) , K s 2] K s 1 がメモリカード 1 9 0 に対して送信される (ステップ S 6 2 4)。

メモリカード 1 9 0においては、メモリカード 1 9 2 から送信された暗号化データを復号処理部 1 4 1 0 がセッションキー K s 1 により復号化して、メモリカード 1 9 2 の公開暗号化キー K P c a r d (2) およびセッションキー K s 2 を復号抽出する (ステップ S 6 2 6)。このとき、切換えスイッチ 1 4 3 5 では接点 P f が閉じておらず、K s 1 発生回路 1 4 3 2 からのキー K s 1 が復号処理部 1 4 1 0 に与えられている。

20 続いて、メモリカード 1 9 0においては、メモリ 1 4 1 2 から、メモリカード 1 9 0 の公開暗号化キー K P c a r d (1) により暗号化されているライセンスキーキー K c 、ライセンス ID データ L i c e n s e - I D およびユーザ ID データ User - I D が読み出される (ステップ S 6 2 8)。

25 続いて、メモリカード 1 9 0 では、復号処理部 1 4 1 6 が、秘密復号キー K c a r d (1) により、ライセンスキーキー K c 、ライセンス ID データ L i c e n s e - I D 、ユーザ ID データ User - I D を復号処理する (ステップ S 6 3 0)。

メモリカード 1 9 0 のコントローラ 1 4 2 0 は、このようにして復号されたライセンスキーキー K c 、ライセンス ID データ L i c e n s e - I D 、ユーザ ID データ User - I D の値を、レジスタ 1 5 0 0 内のデータ値と置換する (ステップ S 6 3 2)。

さらに、メモリカード190の暗号化処理部1414は、復号処理部1410において抽出されたメモリカード192における公開暗号化キーK Card (2)により、ライセンスキーKc、ライセンスIDデータLicense-ID、ユーザIDデータUser-IDとを暗号化する(ステップS634)。

5 メモリカード190の暗号化処理部1414により暗号化されたデータは、切換えスイッチ1409(接点Pgが閉じている)を介して、さらに、暗号化処理部1406に与えられ、暗号化処理部1406は、データ[Kc, License-ID, User-ID]K Card (2)をメモリカード192のセッションキーKs2により暗号化する(ステップS636)。このとき、切換えスイッチ1435は、接点Pgが閉じており、復号処理回路1410からのセッションキーKs2が暗号化処理部1406に与えられている。

続いて、メモリカード190は、携帯電話機105を介して、メモリカード192に対して、暗号化されたデータ[[Kc, License-ID, User-ID]K Card (2)]Ks2を送信する(ステップS638)。

15 メモリカード192においては、メモリカード190から送信されたデータを復号処理部1410により、セッションキーKs2に基づいて復号化処理して、メモリ1412に格納する(ステップS640)。さらに、メモリカード192は、ライセンスキーK Card (2)に基づいて、データ[Kc, License-ID, User-ID]K Card (2)を復号し、復号されたライセンスIDデータLicense-ID、ユーザIDデータUser-IDをレジスタ1500に格納する(ステップS642)。

一方、メモリカード190は、さらに、レジスタ1500に格納されたライセンスIDデータLicense-IDおよびユーザIDデータUser-IDを消去する(ステップS644)。

25 続いて、メモリカード190は、暗号化コンテンツデータ[Dc]Kcをメモリ1412から読み出し、メモリカード192に対して送信する(ステップS646)。

メモリカード192は、受信した暗号化コンテンツデータをそのままメモリ1412に格納する(ステップS648)。

以上のような処理を行なうと、ステップ S 6 4 4において、ライセンスキー Kc、ライセンス IDデータ *l i c e n s e - I D* およびユーザ IDデータ *User - I D* 等がメモリカード 190 からは消去されているので、メモリカード 190 は「状態 S B」となる。

5 一方、メモリカード 192においては、暗号化コンテンツデータ以外にも、ライセンスキー Kc、ライセンス IDデータ *l i c e n s e - I D*、ユーザ IDデータ *User - I D* 等のすべてのデータが移動されているので、メモリカード 192 は「状態 S A」となっている。

ここで、実施例 7 と同様に、ライセンス IDデータ *l i c e n s e - I D* 等は、
10 レジスター 1500 に格納され、コントローラ 1420 はそれを参照すればよいため、動作に必要な処理量を低減できる。

さらに、セッションキーが、携帯電話機、メモリカードの各々で異なるため、通信のセキュリティーが一層向上する。

ここで、移動時には、再生情報内の再生回数を制限するライセンス IDデータ *L i c e n s e - I D* については、メモリ 1412 に記録されたライセンス ID データ *l i c e n s e - I D* を、レジスター 1500 にて再生の都度修正された再生回数を記録したライセンス IDデータ *l i c e n s e - I D* に変更して、新たな再生情報を構成する。このようにして、メモリカード間をコンテンツデータが移動しても、再生回数に制限があるコンテンツデータの再生回数は、配信時に決められた再生回数の制限を越えることがないようになることが可能である。
20

[実施例 9]

図 3-9 は、実施例 9 のメモリカード 200 の構成を示す概略ブロック図である。

実施例 9 のメモリカード 200 は、以下に説明するように、実施例 8 のメモリカード 190 の構成とは、以下の点で異なることを特徴とする。

25 すなわち、実施例 9 のメモリカード 200 では、実施例 8 のメモリカード 190 の構成において、K media 保持部 1402、K p c a r d (1) 保持部 1405、K c a r d (1) 保持部 1415、[K P m e d i a、C r t t f] K P m a s t e r 保持部 1442、K P m a s t e r 保持部 1450 およびレジスター 1500 が、メモリ 1412 の所定の領域内に設けられる構成となっている。こ

れに応じて、切換えスイッチ 1409 の接点 P_b および P_c が省略され、データベース B_S 4 とメモリ 1412 とは直接データのやり取りを行なわず、メモリ 1412 は、データベース B_S 3 との間でのみデータを授受するものとする。データベース B_S 4 は、データベース B_S 3 を介してメモリ 1412 とデータの授受を行なう。

5 図 40 は、図 39 に示したメモリカード 200 内の記録空間の構成を示す概略図である。メモリカードが独自に管理して、ユーザが自由にその内容を書きかえることも読み出すこともできます、かつ、不当な開封処理に対しては、内部のデータが破壊される TRM モジュールにより構成されるセキュリティー領域 1490 と、ユーザがその内容を自由に読み出し、書き換えが行なえる非セキュリティー領域 1492 を備える。

10 セキュリティー領域 1490 には、メモリカード 200 の出荷時から保持する鍵の保持部、すなわち、K_{media} 保持部 1402、K_{pearl} (1) 保持部 1405、K_{card} (1) 保持部 1415、[K_{Pmedia}、Crtf]K_{Pmaster} 保持部 1442、K_{Pmaster} 保持部 1450 と、平文のライセンス情報が格納されるレジスタ 1500 が設けられる。実施例 8 における図 35 と異なるのは準セキュリティー領域が設けられていない点であり、このため準セキュリティー領域 1491 の格納されていた [K_c、L_{license} - ID、User - ID]K_{card} (1) を K_{card} (1) で復号した平文のライセンスキー K_c、ライセンス ID L_{license} - ID、ユーザ ID User - ID の内、実施例 8 においてレジスタ 1500 に格納されていなかったコンテンツキー K_c もセキュリティー領域 1490 に平文で格納される。このため、実施例 8 に比べてセキュリティー領域 1490 は、より広い記録空間が必要となる。

15 非セキュリティー領域 1493 には、暗号化コンテンツデータ [D_c]K_c が格納され、メモリ 1412 がこれにあたる。したがって、暗号化コンテンツデータ [D_c]K_c は自由に複製することが可能となるが、再生に必要なデータが複製できない構成になっている。

20 また、鍵を保持する全ての鍵保持部をセキュリティー領域に設けるよう説明したが、秘密復号鍵を保持する K_{media} 保持部 1402 および K_{card} (1) 保持部 1415 のみセキュリティー領域に配置さえすれば良く、他の鍵保

持部に保持された鍵は外部より参照できるROM(Read Only Memory)に配置されていても良い。

図4-1は、図3-9で説明したメモリカード200を用いた配信モードを説明するためのフローチャートであり、実施例8の図3-6と対比される図である。

5 図4-1においては、ユーザ1が、メモリカード200を用いることで、コンテンツサーバ1-2からコンテンツデータの配信を受ける場合の動作を説明している。

まず、ユーザ1の携帯電話機105から、ユーザのタッチキー1108の操作等によって、メモリカード200に対して配信リクエストがなされる(ステップS400)。

10 メモリカード200からは、メモリ1412中の[KPmedia,Crtf]KPmaster保持部1442から、携帯電話機105を経由して、コンテンツサーバ1-2に対して、暗号化データ[KPmedia,Crtf]KPmasterが送信される(ステップS402)。

15 コンテンツサーバ1-2においては、暗号化データ[KPmedia,Crtf]KPmasterを受信すると、KPmaster保持部324が保持する公開復号キーKPmasterに基づいて、復号処理部326が復号処理することにより、公開復号キーKPmediaおよび認証データCrtfを取得する(ステップS404)。

20 さらに、コンテンツサーバ1-2においては、認証データCrtfによりメモリカード200の認証を行ない(ステップS406)、メモリカード200が正規のメモリカードであることが証明されれば、処理はS412に移行する。

一方、コンテンツサーバ1-2は、メモリカード200が正規のメモリカードであることが証明されない場合は、配信不許可通知を送信し(ステップS408)、携帯電話機105が配信不許可通知を受信する(ステップS410)。

25 メモリカード200が正規のメモリカードであることが証明された場合、コンテンツサーバ1-2では、セッションキー発生部314が、セッションキーKsを生成する(ステップS412)。

コンテンツサーバ1-2では、続いて、コンテンツサーバ1-2内の暗号化処理部316が、公開暗号化キーKPmediaにより、セッションキーKsを暗号化

処理して、データバスB S 1に与える（ステップS 4 1 4）。

通信装置3 5 0は、暗号化処理部3 1 6からの暗号化セッションキー[K s]K m e d i aを、通信網を通じて、携帯電話機1 0 5のメモリカード2 0 0に対して送信する（ステップS 4 1 6）。

5 メモリカード2 0 0においては、メモリインターフェース1 2 0 0を介して、データバスB S 3に与えられた受信データを、復号処理部1 4 0 4が、データバスB S 3を介してメモリ1 4 1 2から与えられる秘密復号キーK m e d i aにより復号処理することにより、セッションキーK sを復号し抽出する（ステップS 4 1 8）。さらに、メモリカード2 0 0では、K s 1発生部1 4 3 2がセッションキーK s 1を生成する（ステップS 4 2 0）。

続いて、配信モードにおいては、まず、暗号化処理部1 4 0 6は、データバスB S 3を介してメモリ1 4 1 2中のK P c a r d (1)保持部1 4 0 5から与えられる公開暗号化鍵K P c a r d (1)を受け取り、続いて、切換えスイッチ1 4 0 9が接点P aが閉じる状態となっているので、暗号化処理部1 4 0 6は、接点P aを介してK s 1発生部1 4 3 2から与えられるセッションキーK s 1を受け取る。暗号化処理部1 4 0 6は、切換えスイッチ1 4 3 5が接点P eが閉じる状態が選択されているので、復号処理部1 4 0 4からのセッションキーK sにより、公開暗号化鍵K P c a r d (1)およびセッションキーK s 1を暗号化してデータバスB S 3に与える（ステップS 4 2 2）。

20 携帯電話機1 0 5を介して、暗号化処理部1 4 0 6により暗号化されたデータ[K P c a r d (1)、K s 1]K sがコンテンツサーバ1 2に対して送信される（ステップS 4 2 4）。

25 コンテンツサーバ1 2では、通信装置3 5 0により受信され、データバスB S 1に与えられたデータ[K P c a r d (1)、K s 1]K sを復号処理部3 1 8が、セッションキーK sにより復号化処理して、公開暗号化キーK P c a r d (1)およびセッションキーK s 1を復号抽出する（ステップS 4 2 6）。

続いて、配信制御部3 1 2は、ライセンスキーK cを配信情報データベース3 0 4より取得し（ステップS 4 2 8）、かつ、配信情報データベース3 0 4等に保持されているデータを元に、ライセンス1 DデータL i c e n s e - 1 Dおよ

びユーザIDデータUser-ID等のデータを生成する（ステップS430）。

暗号化処理部320は、配信制御部312からのライセンスキーケ_c、ライセンスIDデータLicense-IDおよびユーザIDデータUser-ID等のデータを受取って、復号処理部318より与えられた公開暗号化キーK_{Public} 5 d（1）により暗号化処理する（ステップS432）。

暗号化処理部322は、暗号化処理部320により暗号化されたデータを受取って、さらにセッションキーK_s1により暗号化して、データバスBS1に与え 10 る（ステップS434）。

通信装置350は、暗号化処理部322により暗号化されたデータ[[K_c, 15 License-ID, User-ID] Kcard(1)] K_s1をメモリカード200に対して送信する（ステップS436）。

メモリカード200においては、切換えスイッチ1435が接点P1が閉じる 15 状態が選択される状態に切換えられているので、復号処理部1410は、K_s1 発生部1432からのセッションキーK_s1により、復号処理を行ない、データ [K_c, License-ID, User-ID] Kcard(1)を抽出する（ステップS438）。

さらに、メモリカード200においては、復号処理部1416が、メモリ14 20 12中のKcard(1)保持部1415からの出力に基づいて、復号処理部1410からのデータ[K_c, License-ID, User-ID] Kcard(1)を復号し、復号されたライセンスIDデータLicense-ID、ユーザIDデータUser-ID、ライセンスキーケ_cをメモリ1412中のレジ 25 スタ1500に格納する（ステップS443）。

一方、コンテンツサーバ12は、暗号化コンテンツデータ[D_c] K_cを配信情報データベース304より取得して、通信装置350を介して、メモリカード 180に送信する（ステップS444）。

メモリカード200においては、受信した暗号化コンテンツデータ[D_c] K_cをそのままメモリ1412に格納する（ステップS446）。

以上のような動作により、メモリカード200は、コンテンツデータを再生可能な状態となる。

図4-2は、携帯電話機105内において、実施例9のメモリカード200に保持された暗号化コンテンツデータから、コンテンツデータを復号化し、音楽として外部に出力するための再生処理を説明するフローチャートであり、実施例8の図3-7と対比される図である。

5 図4-1を参照して、携帯電話機のタッチキー1108等からのユーザ1の指示により、再生リクエストが携帯電話機105に与えられると（ステップS500）、携帯電話機105からメモリカード200に対して暗号化データ[Kp, Crtf]Kpmasterが送信される（ステップS502）。

10 メモリカード200では、復号処理部1452での公開復号キーKpmasterによる復号処理により、公開暗号化鍵Kpおよび認証データCrtfが取得される（ステップS504）。コントローラ1420は、認証データCrtfにより携帯電話機105が正規の機器であるかを認証し（ステップS506）、正規の機器であると証明されると、処理をステップS508に移行し、正規の機器であると証明されないと再生不許可の通知を携帯電話機105に対して送信する（ステップS544）。

15 携帯電話機105が正規の機器であると証明された場合（ステップS506）、セッションキー発生部1432がセッションキーKs1を生成する（ステップS508）。暗号化処理部1430は、復号処理部1452からの公開暗号化キーKpに基づいて、セッションキーKs1を暗号化し（ステップS510）、暗号化セッションキー[Ks1]Kpがメモリカード200から携帯電話機105に対して送信される（ステップS512）。

20 携帯電話機105では、復号処理部1522での復号処理により、セッションキーKs1が復号され抽出される（ステップS514）。続いて、セッションキー発生部1502においてセッションキーKsが生成され（ステップS516）、暗号化処理部1504がセッションキーKs1によりセッションキーKsを暗号化して（ステップS518）。携帯電話機105からメモリカード200に対して、暗号化セッションキー[Ks]Ks1が送信される（ステップS520）。

25 メモリカード200では、復号処理部1410がセッションキーKs1により、暗号化セッションキー[Ks]Ks1を復号処理してセッションキーKsを抽出

する（ステップS522）。さらに、メモリカード200では、コントローラ1420がメモリ1412中のレジスタ1500からライセンスIDデータLicense-ID、ユーザIDデータUser-ID等を読出す（ステップS524）。

5 コントローラ1420は、ライセンスIDデータLicense-ID等に含まれる情報に基づいて、ライセンスIDデータLicense-ID中のデータにより指定されるコンテンツデータ（音楽データ）の再生処理の累算数が、再生可能回数の上限値を超えているかいないかを判断し（ステップS526）。再生可能回数を超えていないと判断した場合は、メモリカード200は、再生処理が行われることに応じて、メモリ1412中のレジスタ1500中のライセンスIDデータLicense-IDのうち、再生処理の累算数に関するデータを更新する（ステップS528）。

10 続いて、メモリカード200は、メモリ1412から、ライセンスキーKcを読出し、ステップS522において抽出したセッションキーKsにより、ライセンスキーKcを暗号化し（ステップS532）、暗号化ライセンスキー[Kc]KsをデータバスBS2に与える（ステップS534）。

携帯電話機105の復号処理部1506は、セッションキーKsにより復号化処理を行なうことにより、ライセンスキーKcを取得する（ステップS536）。

15 続いて、メモリカード200は、暗号化コンテンツキー[Dc]Kcをメモリ1412から読出し、データバスBS2に与える（ステップS538）。

携帯電話機の音楽再生部1508は、暗号化コンテンツキー[Dc]Kcを、抽出されたライセンスキーKcにより復号処理し（ステップS540）、コンテンツデータを再生して混合部1510に与える（ステップS542）。

一方、ステップS526において、コントローラ1420が復号処理は不可能であると判断した場合、メモリカード200は、携帯電話機105に対して、再生不許可通知を送信する（ステップS544）。

以上のような構成とすることで、メモリカードおよび携帯電話機が独自のセッションキーを生成する場合でも、ユーザがコンテンツデータを再生できる回数を制限することが可能である。

図4-3は、実施例9の2つのメモリカード間において、コンテンツデータおよびキーデータ等の移動を行なうモードを説明するためのフローチャートであり、実施例8の図3-8と対比される図である。

図4-3を参照して、まず、図4-3においては、携帯電話機105が送信側であり、これと同様の構成を有する携帯電話機107が受信側であるものとする。また、携帯電話機107にも、メモリカード200と同様の構成を有するメモリカード202が装着されているものとする。

携帯電話機105は、まず、受信側の携帯電話機107に挿入されたメモリカード202に対して、移動リクエストを出力する（ステップS600）。

これに応じて、携帯電話機107に装着されたメモリカード202からは、メモリカード200に対して、暗号化データ[KPmedia, Crtf]KPmasterが送信される（ステップS602）。

メモリカード200においては、暗号化データ[KPmedia, Crtf]KPmasterを受信すると、KPmaster保持部1460が保持する公開復号キーKPmasterに基づいて、復号処理部1452が復号処理することにより、公開暗号化キーKPmediaおよび認証データCrtfを取得する（ステップS604）。

さらに、メモリカード200においては、認証データCrtfによりメモリカード202の認証を行ない（ステップS606）、メモリカード202が正規のメモリカードであることが証明されれば、処理はS612に移行する。一方、メモリカード200は、メモリカード202が正規のメモリカードであることが証明されない場合は、移動不許可通知を送信し（ステップS608）、携帯電話機107が移動不許可通知を受信する（ステップS610）。

メモリカード202が正規のメモリカードであることが証明された場合、メモリカード200では、セッションキー発生部1432が、セッションキーKs1を生成する（ステップS612）。

メモリカード200では、続いて、暗号化処理部1430が、公開暗号化キーKPmediaにより、セッションキーKs1を暗号化処理して、データバスB-S3に与える（ステップS614）。

メモリカード200からは、暗号化処理部1430からの暗号化セッションキー[Ks]Kmediaを、携帯電話機105を通じて、携帯電話機107のメモリカード202に対して送信する(ステップS616)。

メモリカード202においては、メモリインターフェース1200を介して、データバスBS3に与えられた受信データを、復号処理部1404が、秘密復号キーKmediaにより復号処理することにより、セッションキーKsを復号し抽出する(ステップS618)。さらに、メモリカード202では、Ks1発生器1432と同様の構成を有するKs2発生部1432'がセッションキーKs2を生成する(ステップS620)。

統いて、メモリカード202では、まず、暗号化処理部1406は、データバスBS3を介してメモリ1412中のKPCard(1)保持部1405から与えられる公開暗号化鍵KPCard(1)を受け取り、切換えスイッチ1409が接点Paが閉じる状態となっているので、暗号化処理部1406は、接点Paを介してKs2発生部1432'から与えられるセッションキーKs2を受け取る。暗号化処理部1406は、切換えスイッチ1435が接点Peが閉じる状態が選択されているので、復号処理部1404からのセッションキーKs1により、公開暗号化鍵KPCard(1)およびセッションキーKs2を暗号化してデータバスBS3に与える(ステップS622)。

携帯電話機107を介して、暗号化処理部1406により暗号化されたデータ[KPCard(1)、Ks2]Ks1がメモリカード200に対して送信される(ステップS624)。

メモリカード200においては、メモリカード202から送信された暗号化データを復号処理部1410がセッションキーKs1により復号化して、メモリカード202の公開暗号化キーKPCard(2)およびセッションキーKs2を復号抽出する(ステップS626)。このとき、切換えスイッチ1435では接点Pfが閉じており、Ks1発生回路1432からのセッションキーKs1が復号処理部1410に与えられている。

統いて、メモリカード200では、メモリ1412中のレジスタ1500から、ライセンスキーKc、ライセンスIDデータLicense-ID、ユーザID

データ User-ID とが読み出される (ステップ S 6 2 9)。

さらに、メモリカード 200 の暗号化処理部 1414 は、復号処理部 1410 において抽出されたメモリカード 202 における公開暗号化キー K_P_c a r d (2) により、ライセンスキー K_c、ライセンス ID データ License-ID、ユーザ ID データ User-ID とを暗号化する (ステップ S 6 3 4)。

メモリカード 200 の暗号化処理部 1414 により暗号化されたデータは、切換えスイッチ 1409 (接点 P_d が閉じている) を介して、さらに、暗号化処理部 1406 に与えられ、暗号化処理部 1406 は、データ [K_c, License-ID, User-ID, User-ID] K_c a r d (2) をメモリカード 202 のセッションキー K_s 2 により暗号化する (ステップ S 6 3 6)。このとき、切換えスイッチ 1435 は、接点 P_g が閉じており、復号処理回路 1410 からのセッションキー K_s 2 が暗号化処理部 1406 に与えられている。

統いて、メモリカード 200 は、携帯電話機 105 を介して、メモリカード 202 に対して、暗号化されたデータ [[K_c, License-ID, User-ID] K_c a r d (2)] K_s 2 を送信する (ステップ S 6 3 8)。

メモリカード 202 においては、メモリカード 200 から送信されたデータを復号処理部 1410 により、セッションキー K_s 2 に基づいて復号化処理する (ステップ S 6 4 1)。さらに、メモリカード 202 は、秘密復号キー K_c a r d (2) に基づいて、データ [K_c, License-ID, User-ID] K_c a r d (2) を復号し、復号されたライセンスキー K_c、ライセンス ID データ License-ID、ユーザ ID データ User-ID をメモリ 1412 中のレジスタ 1500 に格納する (ステップ S 6 4 3)。

一方、メモリカード 200 は、レジスタ 1500 よりライセンスキー K_c、ライセンス ID データ License-ID、ユーザ ID データ User-ID を消去し (ステップ S 6 4 4)、暗号化コンテンツデータ [D_c] K_c をメモリ 1412 から読み出し、メモリカード 202 に対して送信する (ステップ S 6 4 6)。

メモリカード 202 は、受信した暗号化コンテンツデータをそのままメモリ 1412 に格納する (ステップ S 6 4 8)。

すなわち、以上のような構成でも、実施例 8 と同様の動作を実現できる。

なお、以上説明してきた各実施例において、配信データとしてコンテンツデータに付随する非暗号化データ、たとえば、上記音楽データの曲名、実演者（歌手、演奏家等）、作曲家、作詞家等の当該音楽データ（コンテンツデータ）に関する著作権データや音楽サーバ30に対するアクセス情報等を、付加情報D1として暗号化コンテンツデータ併せて配信することも可能である。この付加データD1は、配信、移動、複製においてはコンテンツデータとともに処理され、再生時には分離されてコンテンツデータとは個別にアクセス可能となるように、暗号化コンテンツデータと同じメモリ1412に記録される。

この発明を詳細に説明し示してきたが、これは例示のためのみであって、限定となってはならず、発明の精神と範囲は添付の請求の範囲によってのみ限定されることが明らかに理解されるであろう。

請求の範囲

1. 暗号化コンテンツデータを受けて記録するためのメモリカードであつて、前記メモリカードに対応して予め定められた第1の公開暗号化鍵によって暗号化されたデータを復号化するための第1の秘密復号鍵を保持する第1の鍵保持部(1402)と、前記暗号化コンテンツデータの通信ごとに更新されて配信され、前記第1の公開暗号化鍵によって暗号化された第1の共通鍵を受けて、復号処理するための第1の復号処理部(1404)と、
 - 10 前記メモリカードごとに異なる第2の公開暗号化鍵を保持するための第2の鍵保持部(1405)と、前記第2の公開暗号化鍵を、前記第1の共通鍵に基づいて暗号化し、出力するための第1の暗号化処理部(1406)と、前記第2の公開暗号化鍵で暗号化され、さらに前記第1の共通鍵で暗号化されたコンテンツキーを受け、前記第1の共通鍵に基づいて復号化するための第2の復号処理部(1410)と、前記第2の復号処理部の出力を受けて、格納するための第1の記憶部(1412)と、前記第2の公開暗号化鍵によって暗号化されたデータを復号化するための第2の秘密復号鍵を保持する第3の鍵保持部(1415)と、前記第1の記憶部に格納されたデータに基づいて、前記第2の秘密復号鍵により前記コンテンツキーを復号するための第3の復号処理部(1416)とを備える、メモリカード。
2. 前記第1の記憶部は、前記コンテンツキーに基づいて復号できる前記暗号化コンテンツデータを受けて格納する、請求項1記載のメモリカード。
3. 前記メモリカードは、外部から指示される動作モードに応じて、前記メモリカードの動作を制御するための制御部(1420)をさらに備え、前記第1の暗号化処理部は、前記制御部に制御されて、前記コンテンツデータ

の再生動作が指示されるのに応じて、前記第3の復号処理部からの前記コンテンツキーを受けて、前記第1の共通鍵に基づいて暗号化して出力し、

前記第1の記憶部は、前記制御部に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記暗号化コンテンツデータを出力する、請求項
5 2記載のメモリカード。

4. 前記第2の復号処理部は、前記第2の公開暗号化鍵で暗号化され、さらに前記第1の共通鍵で暗号化されて、前記コンテンツキーとともに配信されるライセンス情報データを受け、前記第1の共通鍵に基づいて復号し、

前記第3の復号処理部は、前記第2の復号処理部から与えられる、第1の共通鍵について復号され前記第2の公開暗号化鍵については暗号化された状態の前記ライセンス情報データを復号し、

前記第3の復号処理部からの復号された前記ライセンス情報データを格納するための第2の記憶部（1500）をさらに備える、請求項3記載のメモリカード。

5. 前記メモリカードは、

前記メモリカードに対応して予め定められた第1の公開暗号化鍵を保持し、外部に出力可能な第4の鍵保持部（1440）をさらに備える、請求項1記載のメモリカード。

6. 前記第1の記憶部は、前記コンテンツキーに基づいて復号できる前記暗号化コンテンツデータを受けて格納する、請求項5記載のメモリカード。

20 7. 前記メモリカードは、

外部から指示される動作モードに応じて、前記メモリカードの動作を制御するための制御部をさらに備え、

前記第1の暗号化処理部は、前記制御部に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記第3の復号処理部からの前記コンテンツキーを受けて、前記第1の共通鍵に基づいて暗号化して出力し、

前記第1の記憶部は、前記制御部に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記暗号化コンテンツデータを出力する、請求項
6記載のメモリカード。

8. 前記第2の復号処理部は、前記第2の公開暗号化鍵で暗号化され、さらに前

記第1の共通鍵で暗号化されて、前記コンテンツキーとともに配信されるライセンス情報データを受け、前記第1の共通鍵に基づいて復号し、

前記第3の復号処理部は、前記第2の復号処理部から与えられる、第1の共通鍵について復号され前記第2の公開暗号化鍵については暗号化された状態の前記ライセンス情報データを復号し、

前記第3の復号処理部からの復号された前記ライセンス情報データを格納するための第2の記憶部をさらに備える、請求項7記載のメモリカード。

9. 前記メモリカードは、

第2の共通鍵を生成するキーデータ生成部と、

前記第2の共通鍵を、前記第1の公開暗号化鍵によって暗号化するための第2の暗号化処理部とをさらに備え

暗号化された前記第2の共通鍵は、前記メモリカードから前記他のメモリカードに送信される。請求項1記載のメモリカード。

10. 前記メモリカードは、

少なくとも前記第1の暗号化処理部と、前記第1の復号処理部と、前記第2の復号処理部と、前記第3の復号処理部とが設けられ、第三者には読み出不可能なセキュリティ領域（TRM）と、

前記第1の記憶部が設けられ、第三者に読み出可能なデータ領域とを備える、請求項2または6記載のメモリカード。

11. 前記メモリカードは、

少なくとも前記第1の暗号化処理部と、前記第1の復号処理部と、前記第2の復号処理部と、前記第3の復号処理部と、前記第2の記憶部とが設けられ、第三者には読み出不可能なセキュリティ領域と、

前記第1の記憶部が設けられ、第三者に読み出可能なデータ領域とを備える、請求項4または8記載のメモリカード。

12. 前記第1の記憶部は、前記暗号化コンテンツデータに付随した非暗号化データを、前記暗号化コンテンツデータとともに受け格納する請求項2または6記載のメモリカード。

13. 暗号化データと前記暗号化データを復号するための復号情報データを受け

て記録するためのメモリカードであって、

前記暗号化データを格納する第1の記憶部（1412）と、

前記メモリカードに対応して予め定められた第1の公開暗号化鍵と自身の認証データとを公開認証鍵により復号できるように暗号化して保持し、外部に対して出力可能な第1の鍵保持部（1442）と、

第1の公開暗号化鍵によって暗号化されたデータを復号化するための第1の秘密復号鍵を保持する第2の鍵保持部（1402）と、

前記復号情報データの通信ごとに更新されて送信され、前記第1の公開暗号化鍵によって暗号化された前記第1の共通鍵を受けて、復号処理するための第1の復号処理部（1404）と、

前記メモリカードごとに異なる第2の公開暗号化鍵を保持するための第3の鍵保持部（1405）と、

前記復号情報データの通信ごとに更新される第2の共通鍵を生成するセッションキー発生部（1432）と、

前記第2の公開暗号化鍵と前記第2の共通鍵を、前記第1の共通鍵に基づいて暗号化し、出力するための第1の暗号化処理部（1406）と、

外部にて前記第2の公開暗号化鍵によって暗号化され、さらに第2の共通鍵によって暗号化された前記復号情報データを前記第2の共通鍵に基づいて復号するための第2の復号処理部（1410）と、

前記第2の復号処理部の出力である前記第2の公開暗号化鍵によって暗号化された前記復号情報データを格納する第2の記憶部（1500）と、

前記第2の公開暗号化鍵によって暗号化されたデータを復号するための第2の秘密復号鍵を保持する第4の鍵保持部（1415）と、

前記第2の記憶部に格納されたデータを前記第2の秘密復号鍵に基づいて復号し、前記復号情報データを抽出するための第3の復号処理部（1416）とを備える、メモリカード。

1.4. 前記メモリカードは、

前記公開認証鍵を保持する第4の鍵保持部（1450）と、

前記公開認証鍵によって復号できるように暗号化された外部から与えられる自

身以外の第3の公開暗号化鍵と、自身以外の第2の認証データを復号して抽出する第4の復号処理部（1452）と、

前記第4の復号処理部により抽出された前記第2の認証データに基づいて認証処理を行ない、認証できない場合、前記復号情報データの出力を禁止する制御部
5 (1420) と、

前記セッションキー生成部にて通信ごとに更新した第2の共通鍵を、前記第3の公開暗号化鍵に基づいて暗号化して出力する第3の暗号化処理部（1406）と、

外部からの自身以外の固有の第4の公開暗号化鍵に基づいて暗号化を行なうための第3の暗号処理部（1414）をさらに備え、

外部からの復号情報データの出力要求があり、かつ、前記制御部が復号情報データの出力を禁止しない場合、

1) 前記第2の復号処理部は、第2の共通鍵によって暗号化された前記第1の共通鍵、または第4の公開暗号化鍵および第1の共通鍵をさらに復号出力し、

15 (ii) 前記第2の復号処理部にて前記第4の公開暗号化鍵が抽出された場合、前記第3の復号手段は、前記第1の記憶部に記録されたデータから復号情報データを抽出し、前記第3の暗号化処理部は、前記第3の復号処理部の出力を前記第2の復号処理部にて出力された第4の公開暗号化鍵にて暗号化して、さらに、第1の暗号化処理部は、第3の暗号化処理部の出力を前記第2の復号処理部にて抽出された第2の共通鍵に基づいて暗号化して出力し、

20 (iii) 前記第2の復号処理部にて前記第2の共通鍵のみが抽出された場合、前記第2の復号処理手段は、前記第1の記憶部に格納されたデータから復号情報データを抽出し、前記第3の暗号化処理部は、前記第2の復号処理部の出力を、前記第2の復号処理部にて抽出された第2の共通鍵に基づいて暗号化出力する、請求項13記載のメモリカード。

25 15. 前記復号情報データは、前記復号情報データのメモリカードからの出力を制御するためのアクセス制御データをさらに含み、

前記第3の復号部にて前記第2の公開暗号化鍵によって暗号がされた復号再生情報から抽出した前記アクセス制御情報を格納する第3の記憶部をさらに備え、

前記制御部は、前記第3の記憶部に格納された前記アクセス制御データに基づいて復号情報データの出力を禁止する、請求項1-4記載のメモリカード。

1.6. 前記メモリカードの記録空間は、

第三者に読み出不能かつ書き不可能なセキュリティ領域と、

5 第三者に読み出可能であり、格納データはメモリカード固有の暗号化が施されている準セキュリティ領域と、

第三者に読み出および書き可能な非セキュリティ領域とに区分され、

前記セキュリティ領域は、前記第1、第3の録保持部および第3の記憶部を含み、

10 前記準セキュリティ領域は、前記第2の記憶部を含み、

前記非セキュリティ領域は、第1の記憶部を含む、請求項1-5記載のメモリカード。

1.7. 前記準セキュリティ領域および前記非セキュリティ領域は、同一メモリ上に配置される請求項1-6記載のメモリカード。

15 1.8. 暗号化データと前記暗号化データを復号するための復号情報データを受けて記録するためのメモリカードであつて、

ERROR: stackunderflow
OFFENDING COMMAND: ~

STACK: